INTERNATIONAL CYBERSECURITY AND DIGITAL FORENSICS ACADEMY

Lab Title: Mobile and Cloud Forensics

Course Code: ACI801 Lab Exercise-2

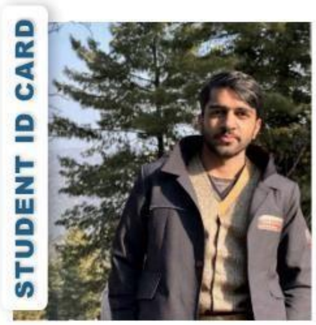
Student Name: Ahtisham Tanveer

Student ID: 2025/ACI/9979

Programme Name: Advance Cybercrime Investigations

Instructor Name: Aminu Idris

Date of submission: 08/09/2025



AHTISHAM TANVEER
2025/ACI/9979
CYBERCRIME INVESTIGATIONS

Exp Date: **November, 2025**

Executive Summary

This lab exercise focused on performing mobile device and cloud evidence acquisition, analysis, and correlation in a simulated corporate espionage investigation. Using Android Virtual Devices (AVDs) and test cloud accounts, both logical and physical acquisitions were attempted. Extracted data was analyzed for communications, location history, application usage, and cloud artifacts.

Root access and targeted data pulls allowed recovery of relevant files, including messages, email metadata, browsing history, and synced cloud storage evidences.

I have used windows CMD and ADB for Logical acquisition. For forensics purpose tools like Autopsy and SQLite Database browser (logical acquisition).

Lab Objectives

- Set up a mobile forensic environment using emulated devices and cloud accounts.

- Perform logical and attempted physical acquisitions of Android device data.

- Analyze mobile communication, location, and application artifacts.

- Collect and analyze evidence from Google Drive, Dropbox, and OneDrive etc.

- Address legal, technical, and encryption-related challenges in mobile/cloud forensics.

Tools and Resources Used

- **Android Studio & AVD Manager** – Suspect (Android 10) and Evidence (Android 12) devices
- **ADB (Android Debug Bridge)** – Logical acquisition, file pulls, and shell access
- **Rooted Emulator Image** – Full file system access
- **SQLite Database Browser** – SMS, WhatsApp, email DB analysis
- **Autopsy** – File system and artifact analysis

Methodology:

- **Environment Setup** – Created AVDs, installed required apps, and configured test accounts.
- **Evidence Simulation** – Populated suspect device with SMS, WhatsApp chats, emails, location check-ins, documents, and deleted files.
- **Logical Acquisition** – Used ADB to pull `/sdcard/` and selected `/data/data/` directories; captured process and network data.
- **Physical Acquisition Attempt** – Rooted emulator and used `dd` to image file system.

←---→

Step by Step Solutions

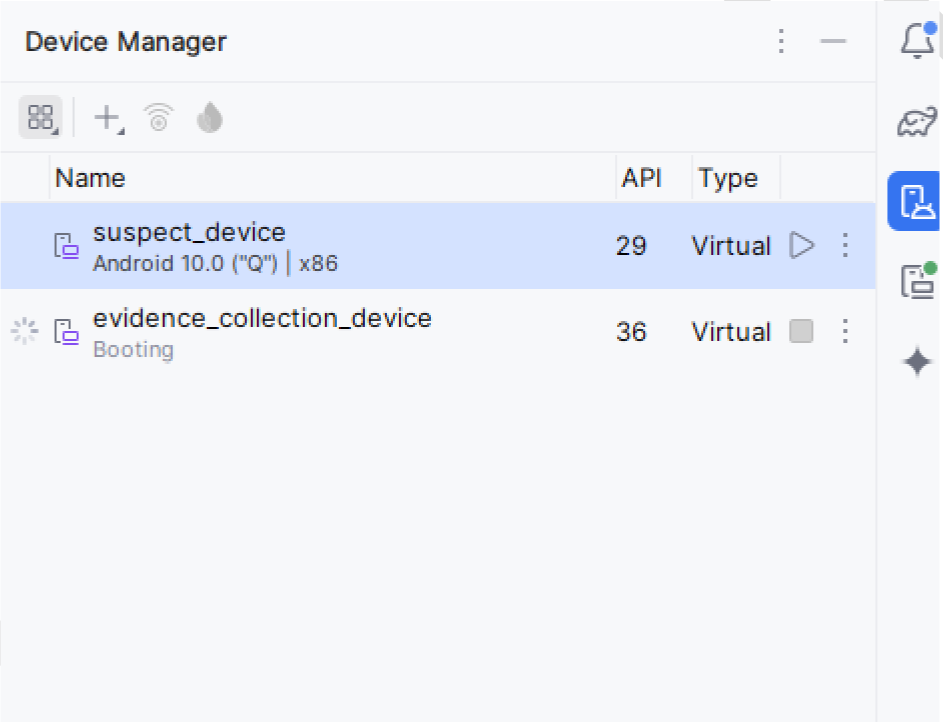
Screen Shots are also attached

Given Below

……

Mobile Device Acquisition:

Case Number	ACI801-LAB2
Evidence Description	Comprehensive acquisition of mobile device data
Date/Time of Acquisition	2025-08-07 10:00 UTC
Acquiring Examiner	AhtishamTanveer
Location	Lab Workstation 02
Evidence Source	Windows



Device Manager

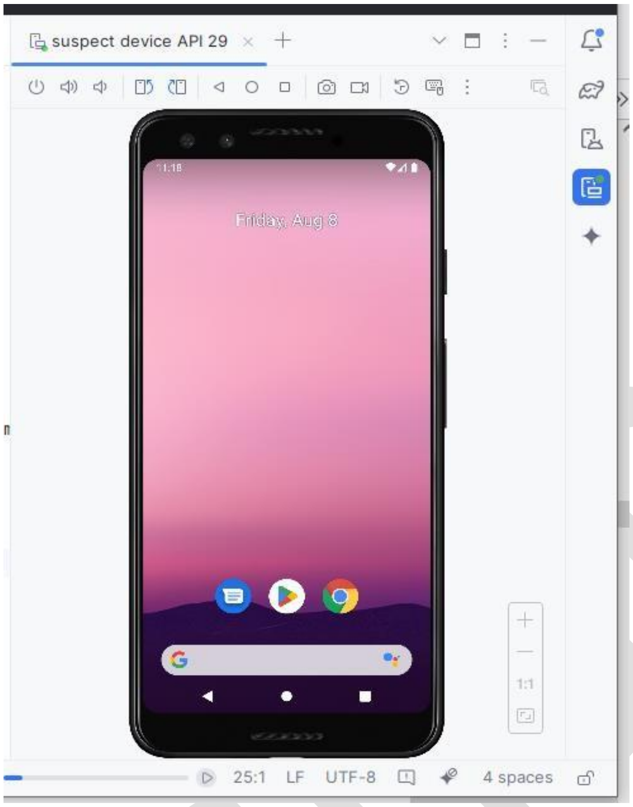
Name	API	Type
suspect_device Android 10.0 ("Q") | x86	29	Virtual
evidence_collection_device Booting	36	Virtual

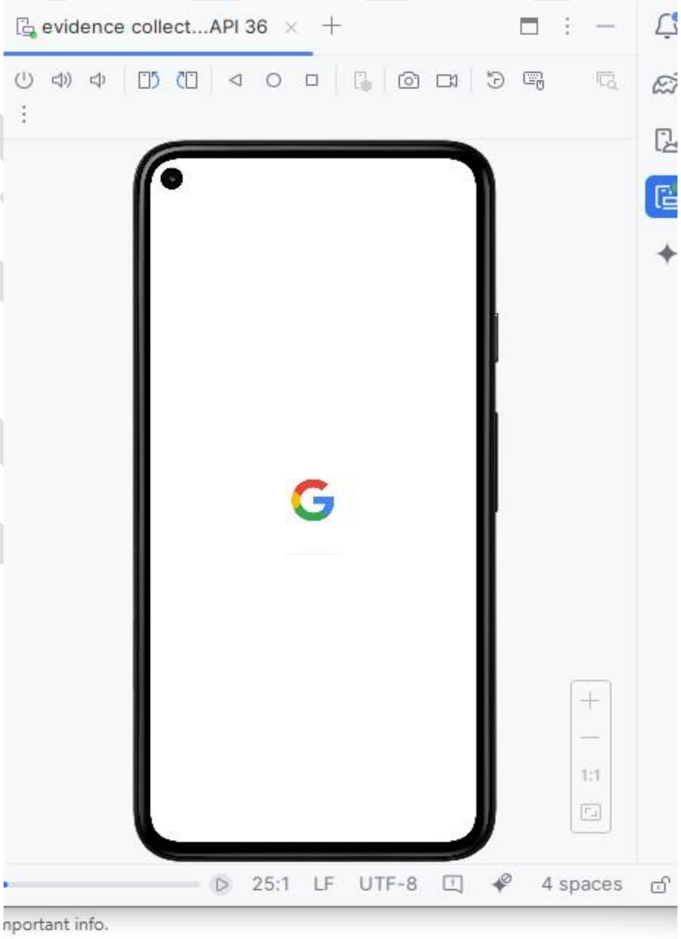
Case Information:

Case Number: ACI801-LAB2

Evidence Number: 002

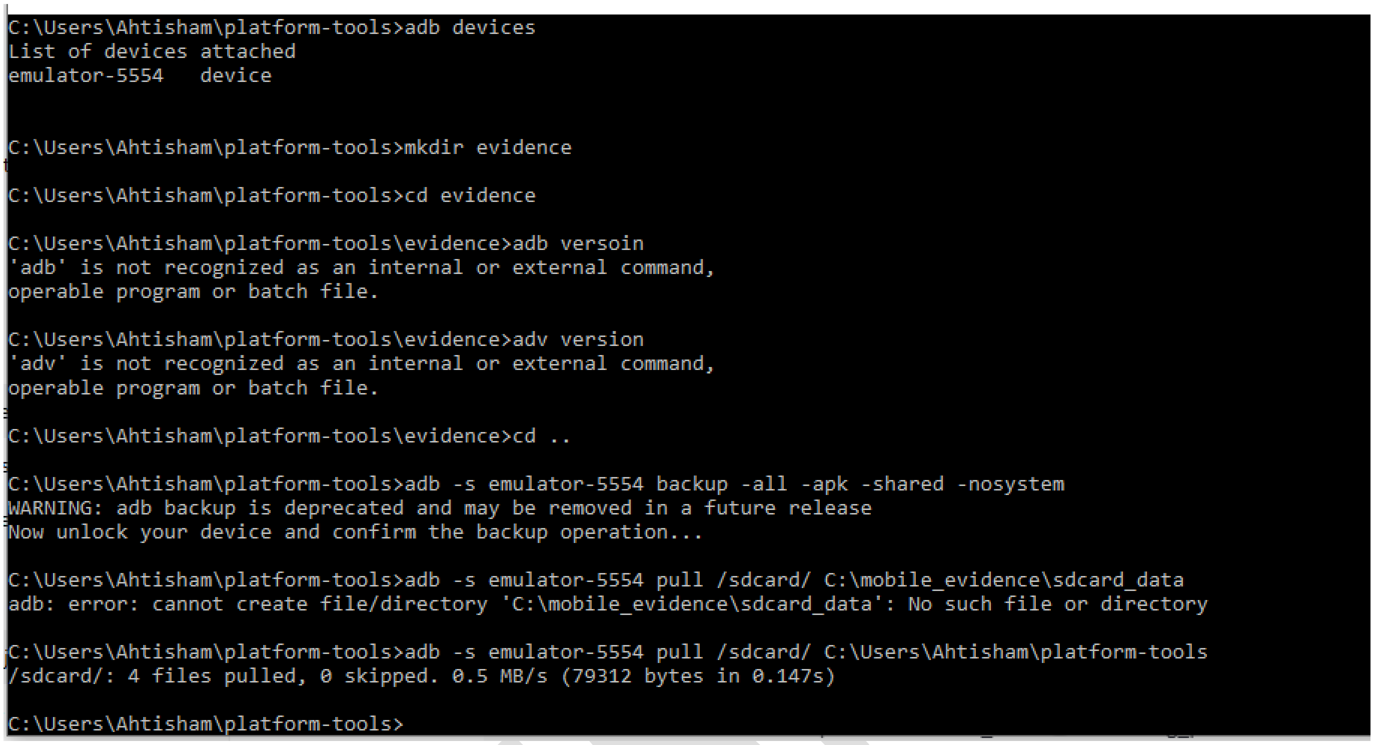
Examiner: AhtishamTanveer


suspect device API 29
1:18
Friday, Aug 8
25:1
LF
UTF-8
4 spaces
1:1


evidence collect...API 36
1:1
25:1
LF
UTF-8
4 spaces
nportant info.

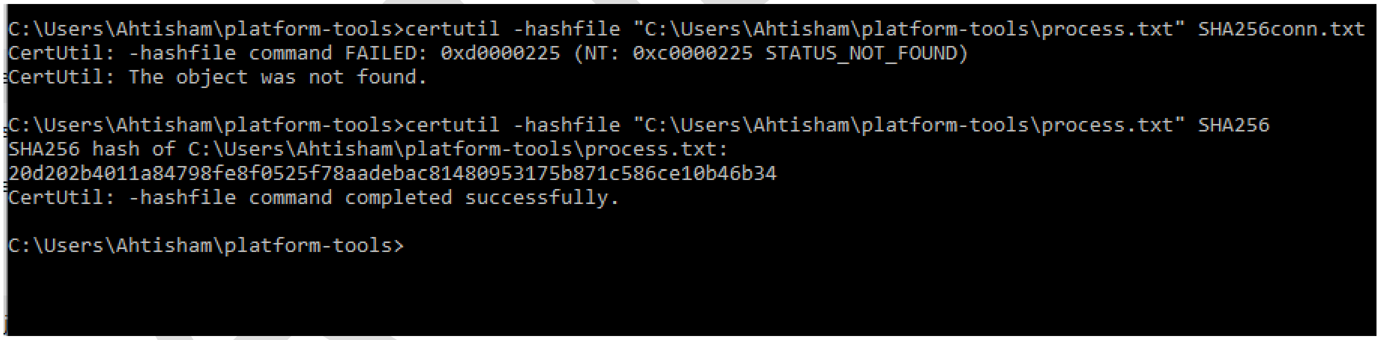
Logical Acquisition Using ADB:

Logical Acquisition of both devices.
First with suspect device.(Cloud data is not included in this device)



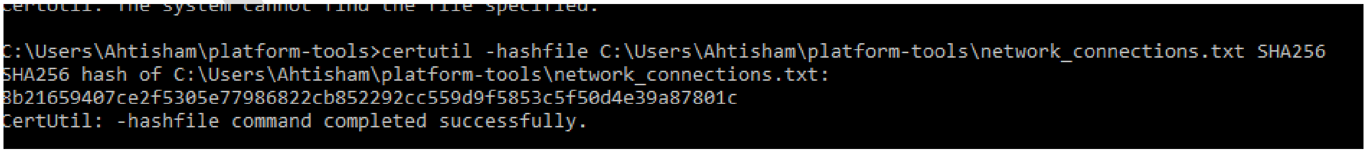
```
C:\Users\Ahtisham\platform-tools>adb devices
List of devices attached
emulator-5554   device


C:\Users\Ahtisham\platform-tools>mkdir evidence

C:\Users\Ahtisham\platform-tools>cd evidence

C:\Users\Ahtisham\platform-tools\evidence>adb versoin
'adb' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Ahtisham\platform-tools\evidence>adv version
'adv' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Ahtisham\platform-tools\evidence>cd ..

C:\Users\Ahtisham\platform-tools>adb -s emulator-5554 backup -all -apk -shared -nosystem
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\Users\Ahtisham\platform-tools>adb -s emulator-5554 pull /sdcard/ C:\mobile_evidence\sdcard_data
adb: error: cannot create file/directory 'C:\mobile_evidence\sdcard_data': No such file or directory

C:\Users\Ahtisham\platform-tools>adb -s emulator-5554 pull /sdcard/ C:\Users\Ahtisham\platform-tools
/sdcard/: 4 files pulled, 0 skipped. 0.5 MB/s (79312 bytes in 0.147s)

C:\Users\Ahtisham\platform-tools>
```

HASHES FOR PROCESSES.TXT:



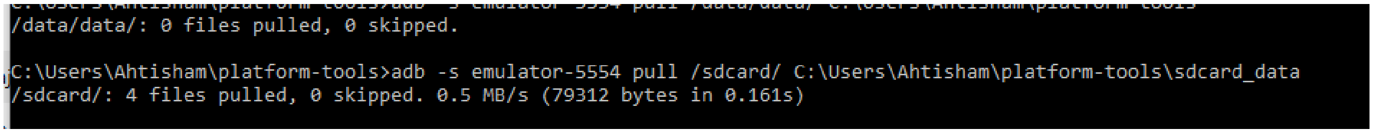
```
C:\Users\Ahtisham\platform-tools>certutil -hashfile "C:\Users\Ahtisham\platform-tools\process.txt" SHA256conn.txt
CertUtil: -hashfile command FAILED: 0xd0000225 (NT: 0xc0000225 STATUS_NOT_FOUND)
CertUtil: The object was not found.

C:\Users\Ahtisham\platform-tools>certutil -hashfile "C:\Users\Ahtisham\platform-tools\process.txt" SHA256
SHA256 hash of C:\Users\Ahtisham\platform-tools\process.txt:
20d202b4011a84798fe8f0525f78aadebac81480953175b871c586ce10b46b34
CertUtil: -hashfile command completed successfully.

C:\Users\Ahtisham\platform-tools>
```

Connections.txt:

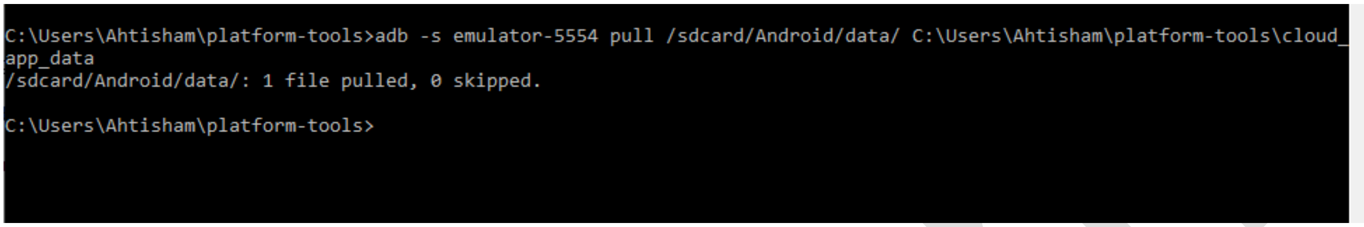


```
certutil: The system cannot find the file specified.

C:\Users\Ahtisham\platform-tools>certutil -hashfile C:\Users\Ahtisham\platform-tools\network_connections.txt SHA256
SHA256 hash of C:\Users\Ahtisham\platform-tools\network_connections.txt:
8b21659407ce2f5305e77986822cb852292cc559d9f5853c5f50d4e39a87801c
CertUtil: -hashfile command completed successfully.
```

Logical data files:

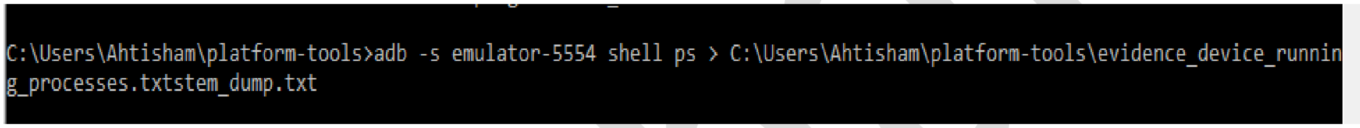


```
C:\Users\Ahtisham\platform-tools>adb -s emulator-5554 pull /data/data/ C:\Users\Ahtisham\platform-tools
/data/data/: 0 files pulled, 0 skipped.

C:\Users\Ahtisham\platform-tools>adb -s emulator-5554 pull /sdcard/ C:\Users\Ahtisham\platform-tools\sdcard_data
/sdcard/: 4 files pulled, 0 skipped. 0.5 MB/s (79312 bytes in 0.161s)
```

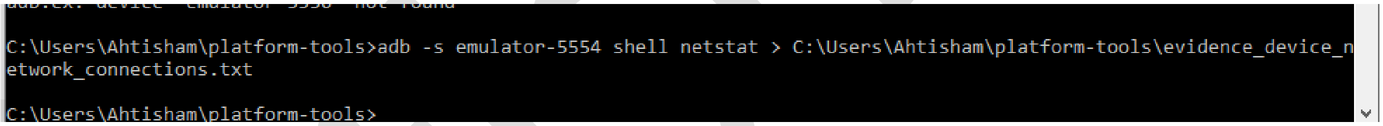


```
C:\Users\Ahtisham\platform-tools>adb -s emulator-5554 pull /sdcard/Android/data/ C:\Users\Ahtisham\platform-tools\cloud_
app_data
/sdcard/Android/data/: 1 file pulled, 0 skipped.

C:\Users\Ahtisham\platform-tools>
```

Evidence Device: (only cloud data is extracted from this device)

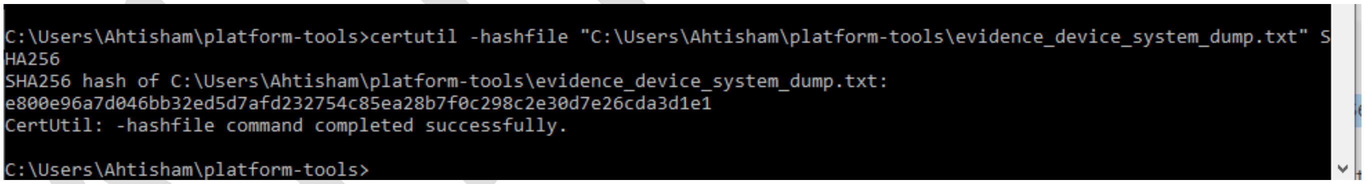


```
C:\Users\Ahtisham\platform-tools>adb -s emulator-5554 shell ps > C:\Users\Ahtisham\platform-tools\evidence_device_runnin
g_processes.txtstem_dump.txt
```

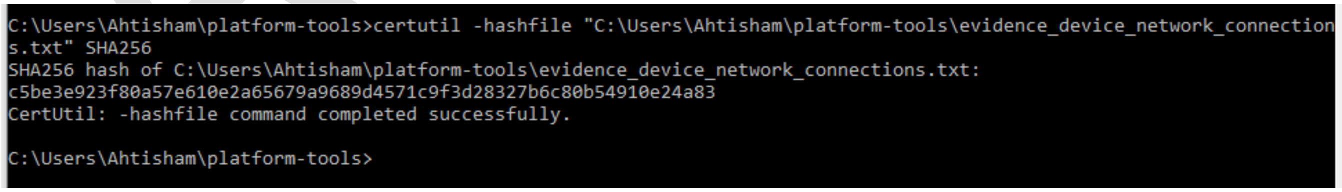


```
adb.exe: device 'emulator-5556' not found

C:\Users\Ahtisham\platform-tools>adb -s emulator-5554 shell netstat > C:\Users\Ahtisham\platform-tools\evidence_device_n
etwork_connections.txt

C:\Users\Ahtisham\platform-tools>
```

Hashes:



```
C:\Users\Ahtisham\platform-tools>certutil -hashfile "C:\Users\Ahtisham\platform-tools\evidence_device_system_dump.txt" S
HA256
SHA256 hash of C:\Users\Ahtisham\platform-tools\evidence_device_system_dump.txt:
e800e96a7d046bb32ed5d7afd232754c85ea28b7f0c298c2e30d7e26cda3d1e1
CertUtil: -hashfile command completed successfully.

C:\Users\Ahtisham\platform-tools>
```



```
C:\Users\Ahtisham\platform-tools>certutil -hashfile "C:\Users\Ahtisham\platform-tools\evidence_device_network_connection
s.txt" SHA256
SHA256 hash of C:\Users\Ahtisham\platform-tools\evidence_device_network_connections.txt:
c5be3e923f80a57e610e2a65679a9689d4571c9f3d28327b6c80b54910e24a83
CertUtil: -hashfile command completed successfully.

C:\Users\Ahtisham\platform-tools>
```

Physical Acquisition Attempt:

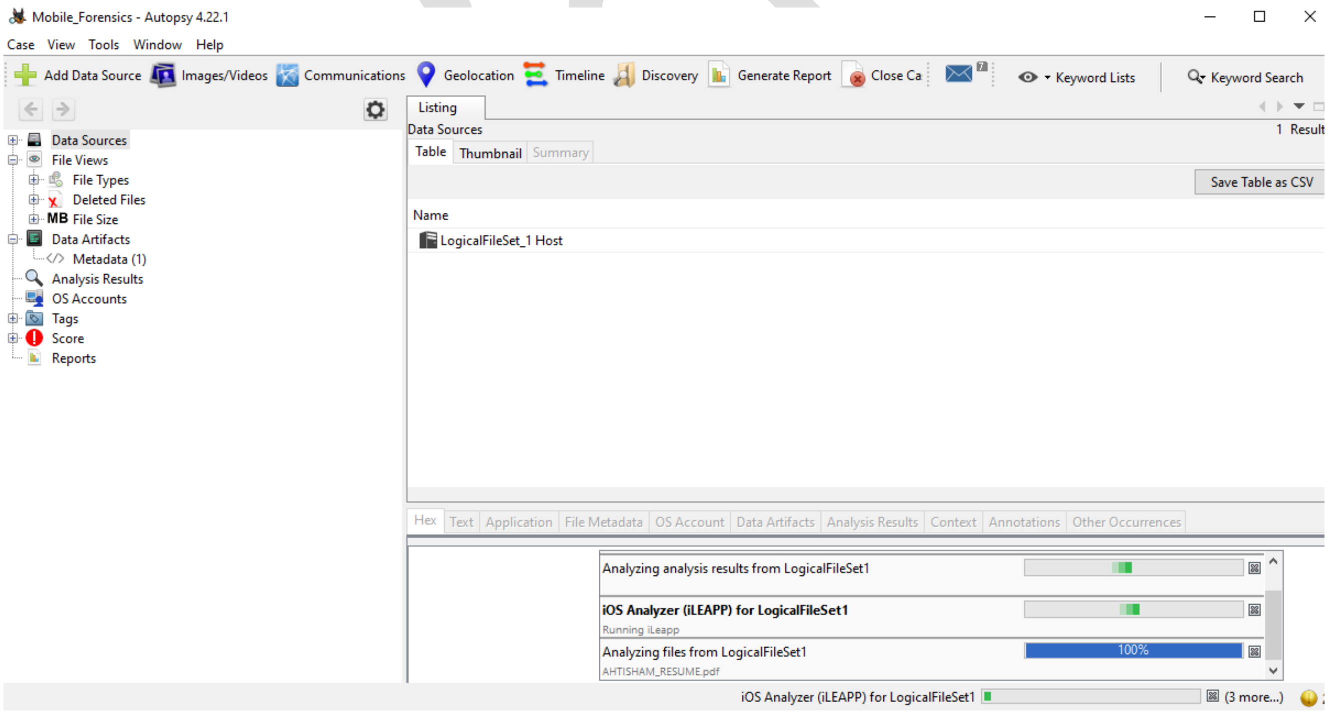
Using Autopsy and SQLite Database browser (.db files)

In real devices like **Pixel 3 or Pixel 5**, physical acquisition methods include:

- Bootloader unlocking
- Using tools like **Cellebrite UFED**, **MSAB XRY**, **Magnet AXIOM**
- Entering **bootloader**, **recovery mode**, or **EDL mode**
- Using `dd` command after rooting

Compare with Logical Acquisition

Type	Logical Acquisition	Physical Acquisition (Attempt)
Tool Used	ADB + Pull	`dd` (requires root)
Device Access Level	User-space	Low-level, raw partitions
Deleted Files	Limited access	Full possibility (if supported)
Emulator Support	✓ Fully supported	✗ Not supported (AVD limitation)



Data Sources — 1 Result

Name
LogicalFileSet_1 Host

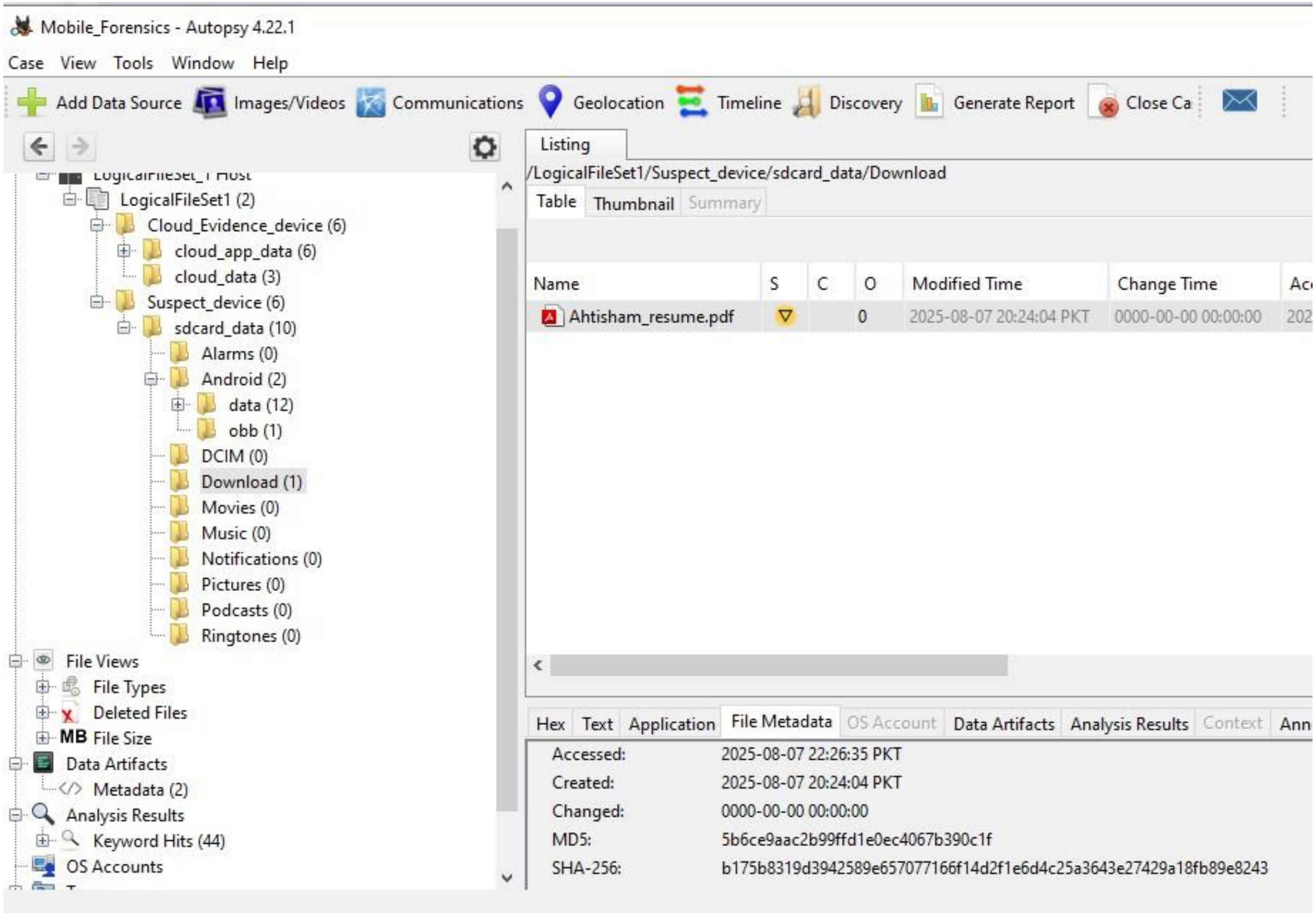
Analyzing analysis results from LogicalFileSet1

iOS Analyzer (iLEAPP) for LogicalFileSet1
Running iLeapp

Analyzing files from LogicalFileSet1 — 100%
AHTISHAM_RESUME.pdf

iOS Analyzer (iLEAPP) for LogicalFileSet1 (3 more...)

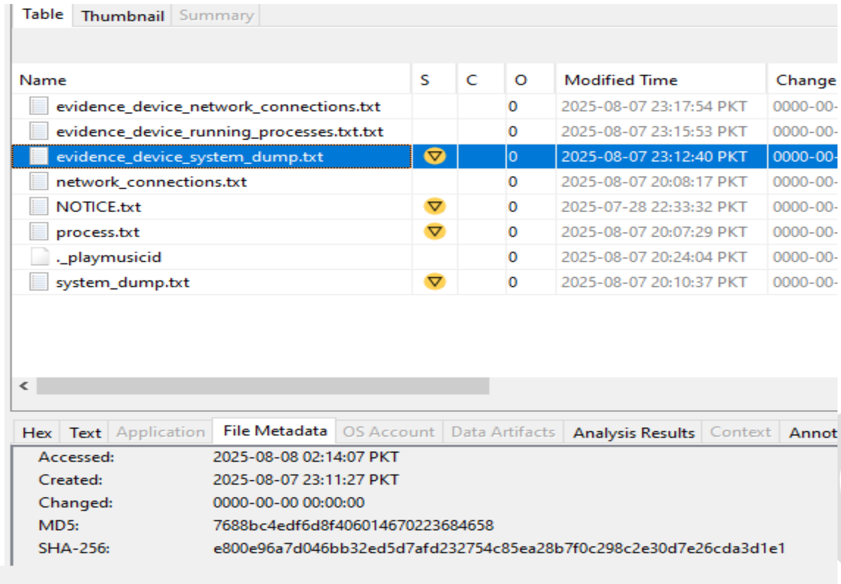
Hashes:



/LogicalFileSet1/Suspect_device/sdcard_data/Download

Name	S	C	O	Modified Time	Change Time	Ac
Ahtisham_resume.pdf	▽		0	2025-08-07 20:24:04 PKT	0000-00-00 00:00:00	202

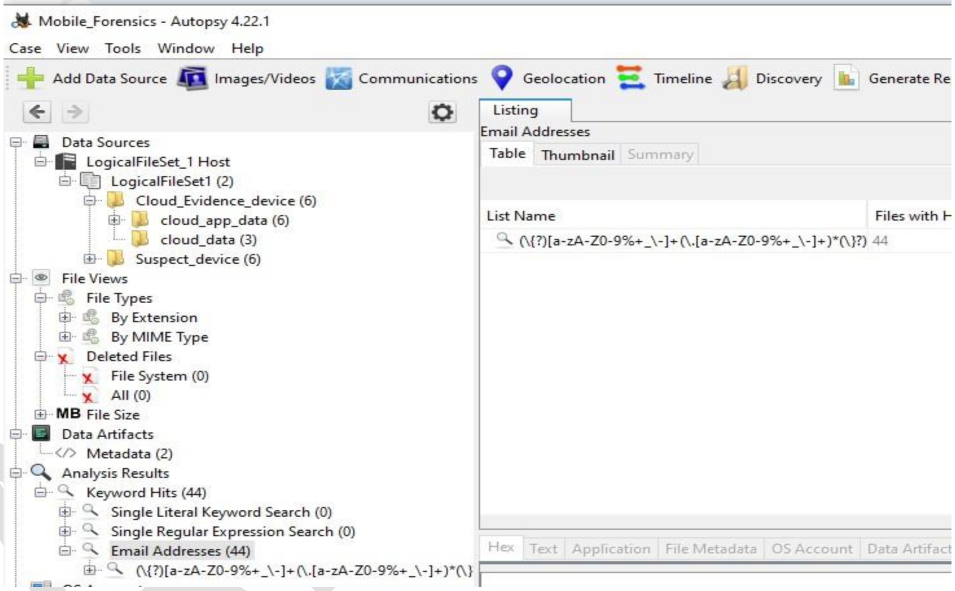
Accessed:	2025-08-07 22:26:35 PKT
Created:	2025-08-07 20:24:04 PKT
Changed:	0000-00-00 00:00:00
MD5:	5b6ce9aac2b99ffd1e0ec4067b390c1f
SHA-256:	b175b8319d3942589e657077166f14d2f1e6d4c25a3643e27429a18fb89e8243



Name	S	C	O	Modified Time	Change
evidence_device_network_connections.txt			0	2025-08-07 23:17:54 PKT	0000-00-
evidence_device_running_processes.txt.txt			0	2025-08-07 23:15:53 PKT	0000-00-
evidence_device_system_dump.txt	▽		0	2025-08-07 23:12:40 PKT	0000-00-
network_connections.txt			0	2025-08-07 20:08:17 PKT	0000-00-
NOTICE.txt	▽		0	2025-07-28 22:33:32 PKT	0000-00-
process.txt	▽		0	2025-08-07 20:07:29 PKT	0000-00-
._playmusicid			0	2025-08-07 20:24:04 PKT	0000-00-
system_dump.txt	▽		0	2025-08-07 20:10:37 PKT	0000-00-

Accessed: 2025-08-08 02:14:07 PKT
Created: 2025-08-07 23:11:27 PKT
Changed: 0000-00-00 00:00:00
MD5: 7688bc4edf6d8f406014670223684658
SHA-256: e800e96a7d046bb32ed5d7afd232754c85ea28b7f0c298c2e30d7e26cda3d1e1

Email Data:

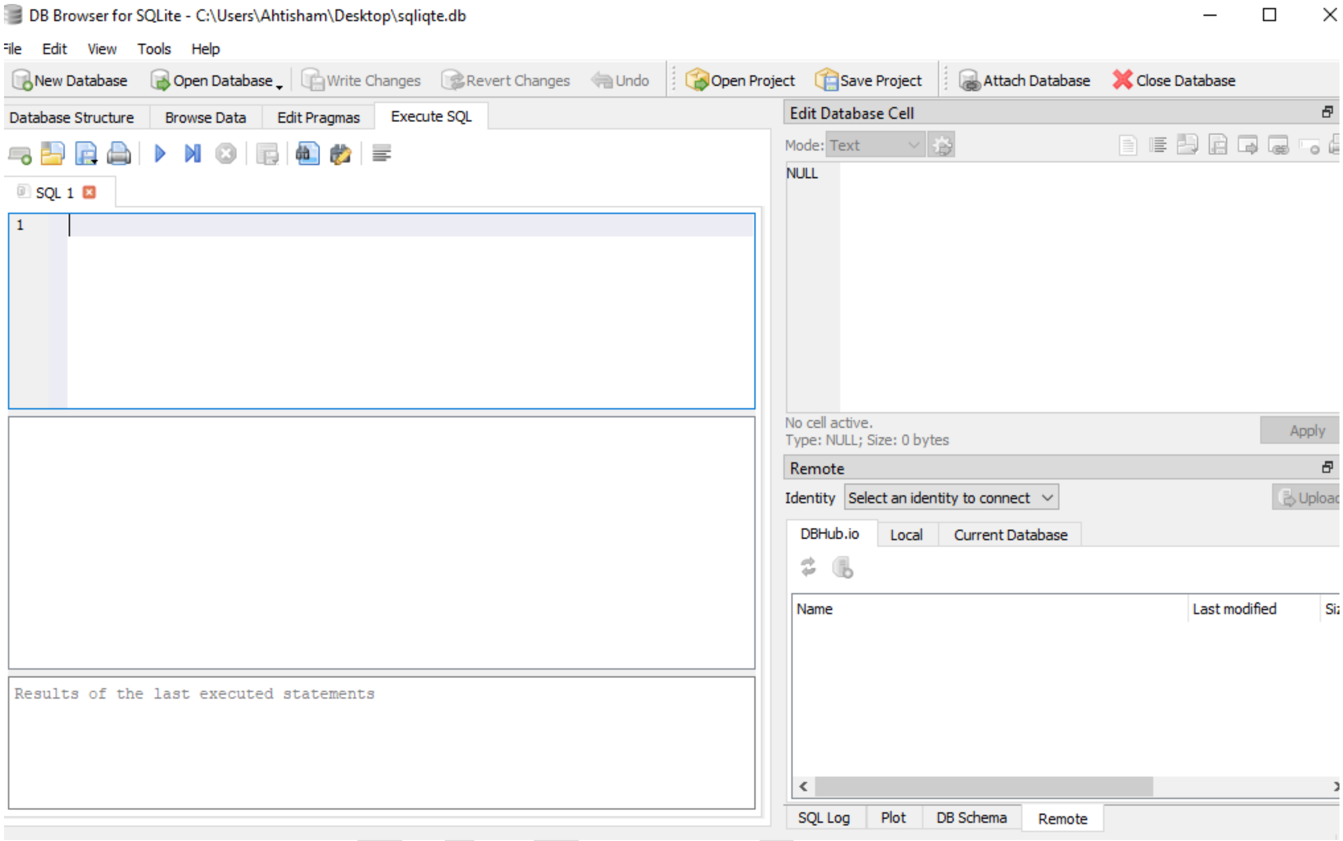


- Data Sources
  - LogicalFileSet_1 Host
    - LogicalFileSet1 (2)
      - Cloud_Evidence_device (6)
        - cloud_app_data (6)
        - cloud_data (3)
      - Suspect_device (6)
- File Views
  - File Types
    - By Extension
    - By MIME Type
  - Deleted Files
    - File System (0)
    - All (0)
  - MB File Size
- Data Artifacts
  - Metadata (2)
- Analysis Results
  - Keyword Hits (44)
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - Email Addresses (44)
      - (\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}

Email Addresses

List Name	Files with H
(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)	44

SQLite DB Browser:



DB Browser for SQLite - C:\Users\Ahtisham\Desktop\sqliqte.db

Mode: Text

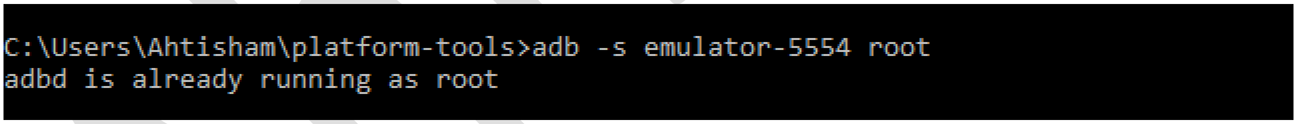
NULL

No cell active.
Type: NULL; Size: 0 bytes

Identity: Select an identity to connect

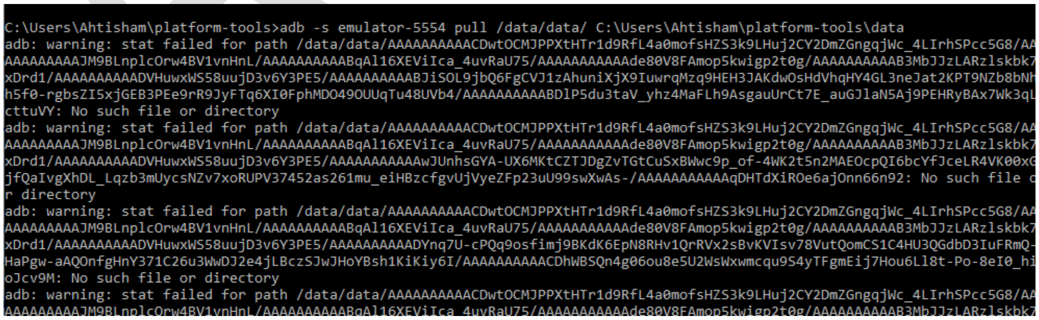
Results of the last executed statements

Running Emulator as a root for accessing data/data files:

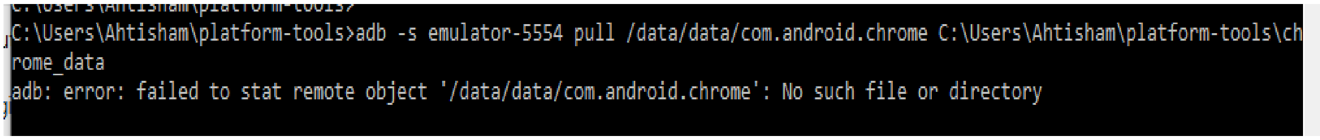


```
C:\Users\Ahtisham\platform-tools>adb -s emulator-5554 root
adbd is already running as root
```

Erros☹:

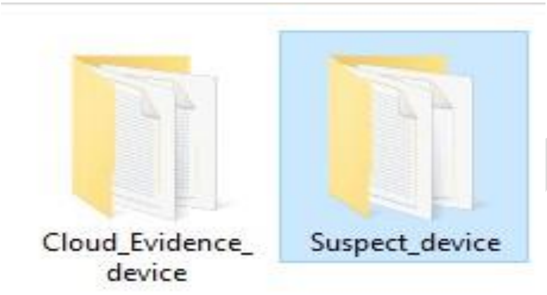


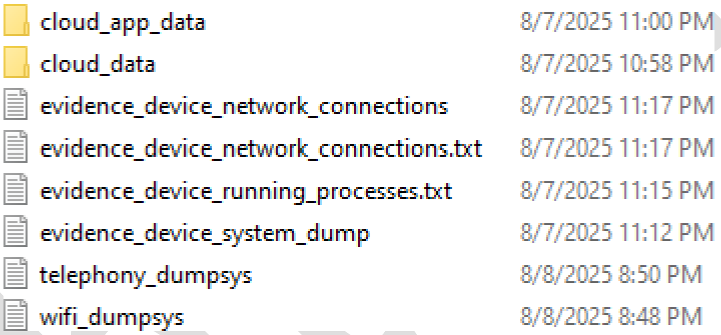
```
C:\Users\Ahtisham\platform-tools>adb -s emulator-5554 pull /data/data/ C:\Users\Ahtisham\platform-tools\data
adb: warning: stat failed for path /data/data/AAAAAAAAAACDwtOCMJPPXtHTr1d9RfL4a0mofsHZS3k9LHuj2CY2DmZGngqjWc_4LIrhSPcc5G8/AA
AAAAAAAAAJM9BLnplcOrw4BV1vnHnL/AAAAAAAAAABqAl16XEViIca_4uvRaU75/AAAAAAAAAAde80V8FAmop5kwigp2t0g/AAAAAAAAAAB3MbJJzLARzlskbk7
xDrd1/AAAAAAAAAADVHuwxWS58uujD3v6Y3PE5/AAAAAAAAAABJiSOL9jbQ6FgCVJ1zAhuniXjX9IuwrqMzq9HEH3JAKdwOsHdVhqHY4GL3neJat2KPT9NZb8bNh
h5f0-rgbsZI5xjGEB3PEe9rR9JyFTq6XI0FphMDO49OUUqTu48UVb4/AAAAAAAAAABDlP5du3taV_yhz4MaFLh9AsgauUrCt7E_auGJlaN5Aj9PEHRyBAx7Wk3qL
cttuVY: No such file or directory
adb: warning: stat failed for path /data/data/AAAAAAAAAACDwtOCMJPPXtHTr1d9RfL4a0mofsHZS3k9LHuj2CY2DmZGngqjWc_4LIrhSPcc5G8/AA
AAAAAAAAAJM9BLnplcOrw4BV1vnHnL/AAAAAAAAAABqAl16XEViIca_4uvRaU75/AAAAAAAAAAde80V8FAmop5kwigp2t0g/AAAAAAAAAAB3MbJJzLARzlskbk7
xDrd1/AAAAAAAAAADVHuwxWS58uujD3v6Y3PE5/AAAAAAAAAAAwJUnhsGYA-UX6MKtCZTJDgZvTGtCuSxBWwc9p_of-4WK2t5n2MAEOcpQI6bcYfJceLR4VK00xG
jfQaIvgXhDL_Lqzb3mUycsNZv7xoRUPV37452as261mu_eiHBzcfgvUjVyeZFp23uU99swXwAs-/AAAAAAAAAAAqDHTdXiROe6ajOnn66n92: No such file o
r directory
adb: warning: stat failed for path /data/data/AAAAAAAAAACDwtOCMJPPXtHTr1d9RfL4a0mofsHZS3k9LHuj2CY2DmZGngqjWc_4LIrhSPcc5G8/AA
AAAAAAAAAJM9BLnplcOrw4BV1vnHnL/AAAAAAAAAABqAl16XEViIca_4uvRaU75/AAAAAAAAAAde80V8FAmop5kwigp2t0g/AAAAAAAAAAB3MbJJzLARzlskbk7
xDrd1/AAAAAAAAAADVHuwxWS58uujD3v6Y3PE5/AAAAAAAAAADYnq7U-cPQq9osfimj9BKdK6EpN8RHv1QrRVx2sBvKVIsv78VutQomCS1C4HU3QGdbD3IuFRmQ-
HaPgw-aAQOnfgHnY371C26u3WwDJ2e4jLBczSJwJHoYBsh1KiKiy6I/AAAAAAAAAACDhWBSQn4g06ou8e5U2WsWxwmcqu9S4yTFgmEij7Hou6Ll8t-Po-8eI0_hi
oJcv9M: No such file or directory
adb: warning: stat failed for path /data/data/AAAAAAAAAACDwtOCMJPPXtHTr1d9RfL4a0mofsHZS3k9LHuj2CY2DmZGngqjWc_4LIrhSPcc5G8/AA
AAAAAAAAAJM9BLnplcOrw4BV1vnHnL/AAAAAAAAAABqAl16XEViIca_4uvRaU75/AAAAAAAAAAde80V8FAmop5kwigp2t0g/AAAAAAAAAAB3MbJJzLARzlskbk7
```



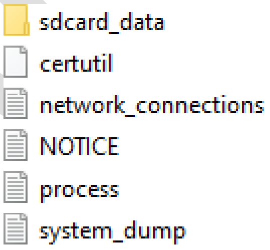
```
C:\Users\Ahtisham\platform-tools>
C:\Users\Ahtisham\platform-tools>adb -s emulator-5554 pull /data/data/com.android.chrome C:\Users\Ahtisham\platform-tools\ch
rome_data
adb: error: failed to stat remote object '/data/data/com.android.chrome': No such file or directory
```

Folders with different data:





```
cloud_app_data                                   8/7/2025 11:00 PM
cloud_data                                       8/7/2025 10:58 PM
evidence_device_network_connections              8/7/2025 11:17 PM
evidence_device_network_connections.txt          8/7/2025 11:17 PM
evidence_device_running_processes.txt            8/7/2025 11:15 PM
evidence_device_system_dump                      8/7/2025 11:12 PM
telephony_dumpsys                                8/8/2025 8:50 PM
wifi_dumpsys                                     8/8/2025 8:48 PM
```



```
sdcard_data
certutil
network_connections
NOTICE
process
system_dump
```

Challenges & Solutions

Challenge	Solution
Could not access /data/data/ due to permission issues	Rooted the emulator to gain full access.
“No such file or directory” errors when pulling packages	Verified package existence using adb shell pm list packages before extraction.
Windows path length & symbolic link errors	Compressed data into .tar.gz before pulling to host system.
Encrypted app databases (Signal, Telegram)	Collected indirect data from notifications, keyboard cache, and linked cloud backups.
Cloud-deleted file recovery	Used cloud service “Version History” and “Deleted Files” recovery tools.

Recommendations

1. **Use Rooted Test Environments** – Rooting allows full access to protected app data during labs.
2. **Validate Package Names Before Extraction** – Run adb shell pm list packages to confirm app presence.
3. **Compress Data Before Transfer** – Use tar to avoid path length issues and maintain directory structure.
4. **Verify Hashes on Both Ends** – Ensure acquisition integrity by checking hash values pre- and post-transfer.
5. **Document Encryption Limitations** – Note encrypted artifacts and pursue alternative evidence sources.
6. **Leverage Cloud Metadata** – Use built-in recovery and version history tools for deleted items.

Conclusion:

The lab successfully demonstrated the complete workflow of mobile and cloud forensics, from acquisition to analysis and reporting. Root access was essential for comprehensive artifact extraction, especially for app data in /data/data/. Combining mobile device artifacts with cloud service logs provided a more complete picture of the suspect’s activities. The exercise reinforced the need for multiple acquisition techniques, proper legal documentation, and correlation of evidence across platforms to build a strong forensic case.

THE END